REMARKS

Claims 25-38 are still pending in this application. No claim amendments have been made.

The Prior Art Problem to be Solved

Claim 25 is a method for assessing the risk of fraud of a financial transaction within a distributed system, and claim 32 claims a distributed risk assessment system for assessing the risk of fraud of a financial transaction.

Prior art fraud detection systems detect fraud by processing transactional data at a central server. Unfortunately, additional data located at the precise source of the transaction is not transmitted to the central server for processing, and thus a complete risk assessment cannot be performed. In other words, performing risk scoring at a single, central location generally does not enable all of the available detail regarding that transaction to be included in the risk assessment.

For example, if a central scoring location receives transactional data indicating a $5,000 purchase of computer equipment, there is no additional data received indicating whether a single item was purchased or whether five $1,000 computers were purchased (even though the purchase of five computers would be considered riskier). This problem is especially prevalent in online transactions. Other examples of at-source data that are typically not sent to a central location to be included in a risk assessment include Web browser information, a TCP/IP address, an e-mail address, server information, etc. The problem to be solved then, is how to include this remote, at source data, in the assessment of risk of a financial transaction.

One solution might be to make a concerted effort to send ALL at-source data from remote locations to a central server for processing. But, this approach is problematic in that it can be difficult to arrange for all the data to be transmitted centrally, the types of data can change thus requiring the central server to adapt to new data fields, and data privacy issues emerge when sensitive information is being sent to a central site.

The Present Invention

Even though technical hurdles exist, the best way to solve this problem is to perform processing and scoring of the transactional data both centrally and on local client computers. But because additional at-source information (that might be sensitive) is now being used at distributed locations to assess risk (and because certain information will be sent from a central location to a distributed location), the data is encrypted and processing is performed on the encrypted data, thus eliminating the possibility of releasing sensitive information. It is further realized that because the data is being processed both centrally and at distributed client locations, that novel techniques for processing the data can be used. It is through a combination of these techniques that the presently claimed invention addresses the above problem.

For example, claim 25 requires that first and second financial transactions are received at a central computer system. These transactions represent a financial transaction for a particular account and a previous transaction for that account. Features are generated for each transaction and the changes between these features are then determined at the central server. As is known to one of skill in the art, use of *features* (or *characteristic variables*) is a known technique of assessing risk based upon sets of data. Before these feature changes are transmitted to a client computer system for further processing claim 25 requires that they are encrypted to prevent the release of any sensitive information.

<u>The Cited Art Distinguished</u>

As explained above and as required by claim 25 (for example), the present invention relates to assessing financial fraud risk within a distributed system and uses analyses of financial transactions and features generated from those transactions to help assess the risk.

The cited reference *Basch et al.* (*Basch*) does disclose predicting financial risk and analysis of financial transactions, but does not disclose the novel techniques claimed such as assessing risk over a distributed system and the generation of features from encryption transactions. For example, the office action at page 3 alleges that *Basch* discloses "assessing a financial fraud risk within a distributed client/server system" as required in the preamble of claim 25. But, *Basch* only shows a centrally located fraud risk protection system 100 that generates features and scores centrally. There is not a central server <u>and</u> a distributed client computer system that are both capable of generating features and scores as is required by claim 25.

Claim 25 also requires "determining feature changes between said first features and said second features at said central computer system." The office action at pages 3-4 alleges that this step is disclosed in the Abstract by determining whether not a score is below a particular threshold. To the contrary, determining a score is not the same as determining changes between features.

Claim 25 also requires "encrypting said feature changes at said central computer system." Encrypting these changes before a score is generated allows these changes to be transmitted securely. The office action alleges at page 4 that this step is disclosed in column 8, lines 40-51. To the contrary, this portion merely uses the phrase "encryption options" and it is clear from this portion that only alerts and scores might be encrypted if they are sent to the various data sinks. There is no disclosure that feature changes are being encrypted. There is a huge difference. Features and feature changes are used to produce a final risk score; encryption of a score is straightforward as the receiver can simply decrypt it at the other end. But, encryption of features is problematic unless a system is capable of operating on such encrypted data to produce a final score. The present invention does include such a capability while *Basch* discloses no such technique.

Claim 25 requires "transmitting said encrypted feature changes from said central computer system to a client computer system." In this fashion, the feature changes are securely transmitted and the encrypted data may be operated on at a client computer system that is capable of operating on encrypted data to produce a risk score. The office action alleges that this step is disclosed in column 8, lines 39-51. To the contrary, there is no disclosure of feature changes being encrypted, let alone these encrypted feature changes being transmitted to a client computer system that is capable of operating upon such encrypted features to generate a score. The action also alleges that this step is disclosed in column 9, lines 38-49 and in column 9, line 62-column 10, line 2. To the contrary, this portion merely discloses that a risk score is delivered to a data sink or a data consumer. Again, disclosing that a final score is transmitted is not the same as transmitting encrypted feature changes from a central system to a client system. Transmitting a final score requires no further processing. Transmitting encrypted feature changes requires a receiving client system capable of operating upon these encrypted features to generate a final score.

Claim 25 further requires "encrypting said current transaction at said client computer system" and "generating local features from said encrypted current transaction at said client computer system." The office action alleges that these steps are shown in column 10, lines 49-58. This portion of *Basch* merely refers to an account issuer database that has encryption options, presumably for storing data. There is no disclosure of encrypting a transaction, and certainly not of generating features from an encrypted transaction.

Claim 25 further requires "comparing said local features to said received feature changes at said client computer system." The action alleges that the step is disclosed in column 9, lines 44-61. This portion only discloses that risk scores are delivered to a transaction authorization system or to a clearing and settlement system. Again, a risk score is entirely different from the features used to generate such a risk score. And, transmitting a risk score is not in the least the equivalent of comparing local features (that have been generated from an encrypted transaction at a local computer) to feature changes (that had been encrypted and delivered from a central computer system).

Claim 25 finally requires "scoring the results of said comparing . . . whereby the risk associated with that current financial transaction is assessed in a distributed manner." Respectively, this step is not disclosed at the cited location. Scoring is not being performed upon a comparison of local features and central features, and risk is not being assessed in a distributed manner through the use of not only a central system that can generate features, but also a local, client system that can generate features.

Claim 32 is a distributed risk assessment system that requires many of the same features as claim 25 and is believed patentable for the same reasons as above. It is requested that rejections of claims 25 and 32 be withdrawn.

The dependent claims add further requirements that also helped to distinguish the claimed invention over the prior art. For example, claim 26 requires that the features incorporate probability information to assist with the risk calculation; claim 30 requires that secondary features are also calculated, transmitted and used by the client computer system.

Consideration of this application and issuance of a Notice of Allowance at an early date are respectfully requested. If the Examiner believes a telephone conference would in any way expedite prosecution, please do not hesitate to telephone the undersigned at (612) 252-3330.

Respectfully submitted,
BEYER WEAVER & THOMAS

Jonathan O. Scott
Registration No. 39,364

BEYER WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778
Telephone: (612) 252-3330
Facsimile: (612) 825-6304